-

Victoria Maniatis
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza,
Suite 500
Garden City, NY 11530
Tel.: 516-741-5600
VManiatis@milberg.com

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

DIANA VIRUET, on behalf of herself and all others similarly situated, Plaintiff, v. COMMUNITY SURGICAL SUPPLY, INC., Defendant.	Civil Action No. **CLASS ACTION COMPLAINT and DEMAND FOR JURY TRIAL**

Plaintiff Diana Viruet ("Plaintiff"), individually and on behalf of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to herself, upon information and belief as to all others, and upon the investigation conducted by their counsel, bring this Class Action Complaint ("Complaint") against Defendant Community Surgical Supply, Inc. ("CSS" or "Defendant") to obtain damages, restitution, and injunctive relief, and in support thereof, state as follows:

NATURE OF THE ACTION

1. This action arises from CSS's failure to properly secure, safeguard, and adequately destroy the sensitive personal identifiable information that was entrusted to it by Plaintiff and Class Members during the course of its business operations. The types of information at issue include, but are not limited to: Plaintiff's and Class Members' names, Social Security numbers, driver's

license or state-issued identification numbers, and financial account numbers (collectively, "Sensitive Information" or "PII").

2. CSS is a clinically-focused home care equipment and service provider that works with medical professionals to provide medical care solutions in the home.

3. Plaintiff and Class Members include current and former customers of CSS as well as current and former customers of a CSS affiliated institution that shared Plaintiff 's and Class Members' PII with CSS during the course of providing health care and any other services.

4. As part of its services, CSS requires that its customers, including Plaintiff and Class Members, provide CSS with their PII, including, but not limited to, full names, addresses, Social Security numbers, driver's license numbers or other government identification numbers, passport numbers, and dates of birth.

5. As a company that maintains the PII of Plaintiff and Class Members, Defendant owed Plaintiff and Class Members numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to keep Plaintiff 's and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

6. Indeed, during the course if its business operations, Defendant expressly and impliedly promised to safeguard Plaintiff 's and Class Members' PII.

7. Furthermore, by obtaining, collecting, using, retaining, and deriving benefit from Plaintiff 's and Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff and Class Members and knew or should have known that it was responsible for safeguarding and protecting Plaintiff 's and Class Members' PII from unauthorized disclosure access, dissemination, or theft.

8. Plaintiff and Class Members provided their PII to CSS with the reasonable expectation of privacy and mutual understanding that CSS would comply with its legal duties, obligations, and representations to keep such information confidential, safe, and secure.

9. Plaintiff and Class Members further reasonably expected and relied upon Defendant to only use their PII for business purposes, implement reasonable retention and data destruction policies, and to make only authorized disclosures of this information.

10. Plaintiff and Class Members would not have paid the amounts of money they paid for Defendant's services, or surrendered their PII, had they known their information would be maintained using inadequate data security and retention systems.

11. CSS's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the Data Breach.

12. Defendant, however, breached its duties, promises, and obligations, and Defendant's failures to honor its obligations increased the risk that Plaintiff 's and Class Members' Sensitive Information would be compromised in the event of a likely cyberattack.

13. Indeed, Defendant's systems did suffer such a fate, and a criminal cyber-attack successfully targeted and accessed Defendant's systems and files that contained Plaintiff 's and Class Members' PII. Upon information and belief, as a result, Plaintiff 's and Class Members' PII was exfiltrated, stolen, disseminated on the Dark Web, and misused to commit identity theft crimes.

14. Plaintiff alleges CSS failed to provide timely, accurate and adequate notice to Plaintiff and Class Members, whose PII was in the possession and control of CSS. Plaintiff and Class Members' knowledge about what personal identifiable information CSS lost, as well as precisely what types of information was unencrypted and in the possession of unknown third

parties, was unreasonably delayed by CSS' unreasonable notification delay of approximately eight months after it first learned of the data breach.

15. On or about July 29,2022, CSS notified state Attorneys General and many customers and other persons about a widespread data breach involving sensitive PII of certain individuals. CSS explained in its required notice letter that it discovered on *October 15, 2021* (over eight months earlier) that it "experienced a data security incident." MMC determined that "an unauthorized party gained access to portions of our digital environment and accessed certain files and data stored in Community Surgical's digital environment," exposing and allowing access to, and acquisition of, the PII for individual customers detailed above ("Data Breach").[1]

16. Presaging the harm that Defendant knew would befall victims of its Data Breach, the Notice Letter also advised Plaintiff and Class Members "to remain vigilant for signs of unauthorized activity by reviewing your financial statements."[2]

17. Notably, while the Data Breach occurred on October 15, 2021 through December 20, 2021, CSS purportedly did not determine what information was accessed until February 4, 2022. Compounding the risk to Plaintiff and Class Members, CSS then failed to promptly notify the impacted individuals – ultimately, sending the data breach notifications over one month later, an unreasonable amount of time from any objective measure.

18. Currently, the full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach are all within the exclusive knowledge and

---

[1] Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/0eb7c75c-3c8c-4eec-850f-0af1faeb51b9/cf9a41ab-4188-4de6-a43e-3fc603ba985b/document.html (last visited August 9, 2022).

[2] *Id*.

control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

19. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to: its failure to design, implement, and maintain reasonable data security systems and safeguards; and/or failure to exercise reasonable care in the hiring, supervision, training, and monitoring of its employees and agents and vendors; and/or failure to comply with industry-standard data security practices; and/or failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action; and/or failure to design, implement and execute reasonable data retention and destruction policies.

20. Upon information and belief, despite its role in managing so much Sensitive Information, Defendant failed to take basic security measures such as adequately encrypting its data or following industry security standards to destroy PII that was no longer necessary for the intended business purpose. Moreover, Defendant failed to recognize and detect that unauthorized third parties had accessed its network in a timely manner to mitigate the harm. Defendant further failed to recognize that substantial amounts of data had been compromised, and more likely than not, had been exfiltrated and stolen. Had Defendant not committed the acts of negligence described herein, it would have discovered the Data Breach sooner – and/or prevented the invasion and theft altogether.

21. In this era of frequent data security attacks and data breaches, particularly in the healthcare industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

22. Upon information and belief, based on the type of sophisticated and malicious criminal activity, the type of PII targeted, Defendant's admission that the PII was accessed, Defendants' admission that Plaintiff and Class Member's PII was in the files that were accessed, reports of criminal misuse of Plaintiff 's and Class Members' data, and reports of PII on the Dark Web following the Data Breach, Plaintiff 's and Class Members' PII was likely accessed, disclosed, exfiltrated, stolen, disseminated, and used by a criminal third party.

23. As a result of the Data Breach, Plaintiff and the Class Members are at an imminent risk of identity theft.

24. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that Plaintiff 's and Class Members' PII was targeted, accessed, and has been disseminated on the Dark Web. Moreover, Class Members have suffered actual identity theft and misuse of their data following the data breach.

25. As Defendant instructed, advised, and warned in its Notice Letters, Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

26. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) invasion of privacy; (b) financial costs incurred mitigating the mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the mitigating the materialized risk and imminent

threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) the loss of benefit of the bargain (price premium damages), to the extent Class Members paid CSS for services; (h) deprivation of value of their PII; and (i) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff 's and Class Members' Sensitive Information.

27. Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of herself and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price premium damages, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

28. Plaintiff brings this Class Action Complaint against Defendant seeking redress for its unlawful conduct, asserting claims for: (a) negligence; (b) negligence *per se*; (c) breach of confidence; (d) intrusion upon seclusion; (e) breach of implied contract; (f) unjust enrichment; (g) violations of New Jersey state consumer protection statutes; and (j) declaratory judgment.

PARTIES

29. Plaintiff Diana Viruet is a citizen of the state of New Jersey and resides in Toms River, New Jersey. Plaintiff is a consumer whose PII was entrusted to and acquired by Defendant. Defendant notified Plaintiff Viruet of the Data Breach and the unauthorized access of her PII by

sending her a Notice of Data Breach letter, dated July 29, 2022. Plaintiff received CSS's Notice of Data Breach letter, dated March 9, 2022, shortly after that date.

30. Defendant Community Surgical Supply, Inc. is a New Jersey corporation, and maintains its principal place of business at 1390 Route 37 W Toms River, New Jersey, 08755-4924.

31. All of Plaintiff's claims stated herein are asserted against CSS and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

32. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one class member is of diverse citizenship from one defendant, there are more than 100 class members nationwide, and the aggregate amount in controversy exceeds $5,000,000, and minimal diversity exists.

33. The District of New Jersey has personal jurisdiction over Defendant named in this action because Defendant is incorporated and has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

DEFENDANT'S BUSINESS AND PROMISES

34. CSS offers specialized healthcare products to patients, nurses, dieticians, and respiratory therapists, including respiratory, enteral nutrition, sleep and infusion therapy products and services. CSS has service location in New Jersey, Pennsylvania, Massachusetts, Maryland, Maine, Ohio, Connecticut, New Hampshire, New York, and Rhode Island. In providing these

services, CSS offers "the industry's most advanced technologies coupled with outcome-based follow up programs."

35. CSS further holds itself out to be "knowledgeable of insurance guidelines and are ready to assist in complex discharges."

36. In the course and scope of its business, CSS collects massive amounts of highly sensitive PII, including but not limited to, full names, Social Security numbers, passport numbers, addresses, dates of birth, and driver's license number and other governmental identification numbers, account numbers, and financial account information.

37. CSS acquired Plaintiff 's and Class Members' PII as part of its medical and healthcare business operations, and CSS collected and stored the PII for commercial gain.

38. As a condition of their using the services of CSS, consumers were obligated to provide CSS with certain sensitive and non-public PII, including their name, date of birth, address, Social Security number, driver's license, telephone number, email address, financial account numbers, and payment card numbers.

39. Plaintiff and Class Members entrusted their PII to CSS, or CSS affiliate, on the premise and with the understanding that CSS would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties, and/or only retain PII for necessary business purposes and for a reasonable amount of time.

40. CSS has acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, retaining, and protecting PII is vital to many of CSS's business purposes. CSS also makes public representations on its website regarding the value of PII it collects from its customers and users:

> Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only as described below controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.[3]

41. For example, with respect to the privacy of the sensitive PII health information it collects, CSS states in its Privacy Policy that:

> We will use and disclose your health information when we are required to do so by federal, state or local law.
>
> We require any business associates to protect the confidentiality of your information and to use the information only for the purpose for which the disclosure is made. We do not provide customer names and addresses to outside firms, organizations, or individuals except in furtherance of our business relationship with you or as otherwise allowed by law.
>
> We restrict access to nonpublic information about you to those employees who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your personal information.[4]

42. With respect to privacy in general, CSS states that it is "we know that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. ."[5]

43. Plaintiff and the Class Members, as current and former CSS customers and current and former customers of a CSS affiliate, relied on Defendant's express and implied promises and on CSS as a sophisticated entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, to implement reasonable retention policies, to limit access to authorized individuals, and to make only authorized disclosures of this information.

---

[3] CSS, Privacy Statement, https://resources.communitysurgical.com/hc/en-us/articles/7089073233431-Privacy-Policy (last accessed August 12, 2022).

[4] *Id.*

[5] *Id.*

THE DATA BREACH AND DEFENDANT'S RESPONSE

44. Beginning on or about July 29, 2022, CSS notified many of its customers, former customers, customers and former customers of a CSS affiliates, and state Attorneys Generals about a widespread data breach involving sensitive PII of certain current and former customers and customers and former customers of a CSS affiliates.

45. Through an investigation, CSS determined that a third-party criminal or criminals accessed its systems on October 15, 2021.[6] The investigation further determined that Plaintiff 's and thousands of Class Members' PII were present within the files that were accessed.

46. Upon information and belief, the PII was not encrypted or was not adequately encrypted prior to the data breach.

47. The confidential information that was accessed without authorization included full names, Social Security numbers, passport numbers, addresses, dates of birth, and driver's license number and other governmental identification numbers.[7]

48. In response to the Data Breach, rather than promptly inform its customers and employees, CSS waited for over *8 months* after the discovery of the Data Breach, until July 29, 2022 to issue notice. Even then, CSS did not fully disclose the scope of the Data Breach but opted to instead issue a vague letter leaving the Plaintiff and Class Members without a full understanding of how the breach occurred or what happened to their PII once it was accessed. For example, the latter fails to mention or provide any conclusive determination as to whether or not the information was exfiltrated, stolen or taken during the Data Breach, a fact that Plaintiff and Class Members are

[6] July 29, 2022 Letter.

[7] *Id.*

entitled to know and one which would allow them to better mitigate the consequences of Defendant's failure to safeguard their information.

49. In fact, there is no indication by CSS that the investigation concluded that Plaintiff's and Class Members' PII was safe or that the Data Breach was limited to a mere viewing of the PII, as opposed to theft or exfiltration. To the contrary, the Notice Letter leaves a strong implication that the PII was not only fully accessed but that the data was likely exfiltrated and disseminated in the Data Breach.

50. Emsisoft, an award-winning malware-protection software company, states that "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, especially during the preliminary stages of an investigation."[8]

51. Consistent with Emsisoft, CSS issued an express warning and advised the impacted individuals of the seriousness of the attack, and that they should "remain vigilant." The Notice Letter further issued specific instructions and mitigation techniques such as "reviewing account statements" for "unauthorized activity" – CSS specifically stated:

> While we do not have any indication that you (sic) information has been misused, we advise you to remain vigilant for signs of unauthorized activity by reviewing your financial accounts.[9]

52. These warnings and instructions are an acknowledgment by CSS that it is not only plausible that the cyber-attackers acquired the PII for criminal purposes, thereby placing the impacted customers at an imminent threat of identity theft and financial fraud – but that the theft

[8] Emsisoft Malware Lab, The chance of data being stolen in a ransomware attack is greater than one in ten (EMSISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

[9] July 29, 2022 Letter

and dissemination and misuse of the PII is the highly probable, if not certain, result of this type of cyberattack.

53. Without the likelihood of dissemination and misuse, and materialization of identity theft, the warnings, and instructions to mitigate the risk would be unnecessary and would cause more harm than good, and Defendant would not have advised such actions that would cost Plaintiff and Class Members time and money unless it believed those actions to be necessary.

54. As an additional line of protection, CSS created and paid for a program that offered identity theft protection to Class Members. Absent an actual, materialized, and imminent threat to the Plaintiff and Class Members, such a program would also have been unnecessary and a waste of Defendant's time and money. Defendant would not have spent resources creating such a program without the likelihood that the Class Member PII was exfiltrated and disseminated in the attack, and that a materialized and imminent risk of identity theft was present for all Class Members. CSS offered:

> … a complimentary identity protection services through Equifax that includes 12 months of credit monitoring.[10]

55. Finally, CSS also acknowledged implementing improvements to its systems stating, "we have implemented additional technical security measures."[11]

56. While CSS admits that enhanced "technical security measures" were required to improve its data security systems, there is no indication based solely on the Notice Letter whether these steps are fully adequate to protect Plaintiff 's and Class Members' PII going forward, as the

[10] *Id.*

[11] *Id.*

source and root cause of the data breach were not disclosed and remain unknown and undiscoverable absent litigation.[12]

57. What is evident and indisputable is that the Data Breach resulted in the unauthorized access of Defendant's systems and files, and that those compromised files contained the PII of Plaintiff and thousands of Class Members, including their names, Social Security numbers, passport numbers, addresses, dates of birth, and driver's license number and other governmental identification numbers.

58. Upon information and belief, the cyberattack was targeted at CSS and Plaintiff 's and Class Members' PII due to CSS's status as a major healthcare home services company that collects valuable personal and financial data on its many customers and its affiliates' customers.

59. Upon information and belief, the cyberattack was expressly designed to gain access to and steal the private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

60. Upon information and belief, criminal hackers exfiltrated, stole, disseminated, and have misused Plaintiff 's and Class Members' PII because of the value in exploiting and stealing the identities of Plaintiff and Class Members.

61. As a result of the Data Breach, the risk of identity theft has materialized, and Plaintiff and Class Members are at an imminent risk of identity theft.

[12] *Id.*

THE DATA BREACH WAS FORESEEABLE

62. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII preceding the date of the breach.

63. In 2021 alone, there were over 200 data breach incidents.[13] These approximately 200 data breach incidents have impacted nearly 15 million individuals.[14]

64. In light of recent high profile data breaches at other leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), CSS knew or should have known that its systems would be targeted by cybercriminals.

65. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[15]

---

[13] *See* Kim Delmonico, *Another (!) Orthopedic Practice Reports Data Breach*, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/.

[14] *Id*.

[15] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

66. Moreover, it is well known that the specific PII at issue in this case, including social security numbers and financial account information in particular, is a valuable commodity and a frequent target of hackers.

67. As a sophisticated healthcare services entity that collects, utilizes, and stores particularly sensitive PII, CSS was at all times fully aware of the increasing risks of cyber-attacks targeting the PII it controlled, and its obligation to protect the PII of Plaintiff and Class Members.

68. CSS has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

DEFENDANT FAILED TO PROTECT PLAINTIFF 'S AND CLASS MEMBERS' PRIVATE INFORMATION

69. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendant's own acknowledgment of its duties to keep PII private and secure, CSS failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

70. Defendant did not use reasonable security procedures and practices appropriate to the nature of the Sensitive Information it was maintaining for Plaintiff and Class Members, causing the exposure of PII of over 66,000 individuals.

A. Defendant Failed to Properly Comply With Federal Trade Commission Data Security Standards

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

72. The FTC has brought well publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. This includes the FTC's enforcement action against Equifax following a massive data breach involving the personal and financial information of 147 million Americans.

73. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses. There, the FTC advised that businesses should protect the PII that they keep by following some minimum standards related to data security, including, among others:

(a) Encrypting information stored on computer networks;

(b) Identifying network vulnerabilities;

(c) Implementing policies to update and correct any security problems;

(d) Utilizing an intrusion detection systems;

(e) Monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system;

(f) Watching for large amounts of data being transmitted from the system;

(g) Developing a response plan ready in the event of a breach;

(h) Limiting employee and vendor access to sensitive data;

(i) Requiting complex passwords to be used on networks;

(j) Utilizing industry-tested methods for security;

(k) Verifying that third-party service providers have implemented reasonable security measures;

(l) Educating and training employees on data security practices;

(m) Implementing multi-layer security including firewalls, anti-virus, and anti-malware software;

(n) Implementing multi-factor authentication.

74. In particular, the FTC further also advised that companies not maintain PII longer than is needed for authorization of a transaction: "If you don't have a legitimate business need for sensitive personally identifying information, don't keep it."[16]

75. Upon information and belief, CSS failed to implement or adequately implement at least one of these fundamental data security practices.

76. CSS could have prevented this Data Breach by properly following FTC guidelines by adequately encrypting or otherwise protecting its equipment and computer files containing PII.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

B. Defendant Failed to Comply with Industry Standards

78. The healthcare industry also routinely incorporates these cybersecurity practices that are standard in CSS's industry. These minimum standards include but are not limited to:

(a) Maintaining a secure firewall configuration;

(b) Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

(c) Monitoring for suspicious or irregular traffic to servers;

(d) Monitoring for suspicious credentials used to access servers;

[16] FTC, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www/ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

(e) Monitoring for suspicious or irregular activity by known users;

(f) Monitoring for suspicious or unknown users;

(g) Monitoring for suspicious or irregular server requests;

(h) Monitoring for server requests for PII;

(i) Monitoring for server requests from VPNs; and

(j) Monitoring for server requests from Tor exit nodes.

79. Upon information and belief, CSS failed to comply with at least one of these minimal industry standards, thereby opening the door to and causing the Data Breach.

80. CSS could have prevented this Data Breach by properly following industry data security standards by adequately encrypting or otherwise protecting its equipment and computer files containing PII.

81. CSS could also have prevented the scale of the Data Breach simply by designing and implementing data retention practices to delete PII that is no longer needed for an ongoing business purpose.

82. CSS had the resources necessary, and reasonable data security alternatives were known and available to CSS that would have prevented the Data Breach, but CSS neglected to adequately evaluate its systems and invest in adequate security measures, despite its obligation to protect its systems and Plaintiff ’s and Class Members’ PII.

THE VALUE OF PII

83. There is both a healthy black market and a legitimate market for the type of PII that was compromised in this action. PII is such a valuable commodity to criminal networks that once the information has been compromised, criminals often trade the information on the “cyber black market” for years.

84. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17]

85. According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

86. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls

---

[17] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[18] Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Mar. 8, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/.

[19] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

> from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

87. The Social Security Administration has further warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, apply for a job using a false identity, open bank accounts, and apply for other government documents such as driver's license and birth certificates.

88. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

89. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[20] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

90. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

91. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x in price on the black market."[22]

92. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of personal information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[23]

93. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.

---

[21] Brian Naylor, *Victims Of Social Security Number Theft Find It's Hard To Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[22] Tim Greene, *Anthem hack: Personal data stolen sells for 10x price of stolen credit card numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[23] Lee Matthews, *Hackers Stole Customer's License Numbers from Geico In Months-Long Breach*, FORBES (Apr. 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658.

> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[24]

94. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[25] However, this is not the case. As cybersecurity experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[26]

95. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent *The New York Times* article.[27]

96. In addition, if a Class Member's Social Security number or driver's license number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

---

[24] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?* (Oct. 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[25] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAGAZINE (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/.

[26] *Id.*

[27] Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021), https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html.

PLAINTIFF AND CLASS MEMBERS SUFFERED FORESEEABLE CONCRETE HARMS

97. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the foreseeable consequences of the PII ending up in the possession of criminals, the risk of identity theft is materialized and imminent.

98. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, reports of misuse of Class Member PII, and reports of dissemination on the Dark Web, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; or file false unemployment claims.

99. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[28] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

100. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. The fraudulent activity resulting from the Data Breach may not become evident for years.

[28] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

101. Indeed, "[t]he risk level is growing for anyone whose information is stolen in a data breach."[29] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[30] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

102. To date, Defendant has done little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this data breach. The complimentary fraud and identity monitoring service offered by Defendant through Experian IdentityWorks is wholly inadequate as the services are only offered for months and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

103. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, in Defendant's words, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

104. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing

---

[29] Susan Ladika, *Study: Data Breaches Pose a Greater Risk*, Fox Business (Mar. 6, 2016), https://www.foxbusiness.com/features/study-data-breaches-pose-a-greater-risk.

[30] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH-IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, Al Pascal, JAVELIN STRATEGY & RESEARCH (June 2014), https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf.

passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

105. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[31]

106. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[32]

107. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant or its clients for services, Plaintiff and other reasonable consumers understood and expected that they were paying for services and data security, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected.

---

[31] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[32] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

108. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the imminent risk of identity theft, Plaintiff and Class Members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) deprivation of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information.

PLAINTIFF'S EXPERIENCE

Plaintiff 's Experience

109. Upon information and belief, Plaintiff Viruet provided her PII to a CSS affiliate who provided the PII to CSS during the course of normal business. Upon information and belief, Plaintiff also paid the CSS or its affiliate a fee for its services.

110. Plaintiff greatly values her privacy and Sensitive Information. Plaintiff has taken reasonable steps to maintain the confidentiality of his PII, and he has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. She does her best to store any and all documents containing sensitive PII in a secure location and destroy any documents she receives in the mail that contain PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts.

111. Plaintiff is extremely careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. She stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

112. In August 2022, Plaintiff received a Notice Letter from CSS, substantially similar to Exhibit 1, informing her that her full name, address, Driver's license or other government identification number, passport number, Social Security number, or date of birth were potentially accessed by unauthorized third parties. In the Notice Letter, CSS advised her to take certain steps to protect her PII and otherwise mitigate her damages. CSS never notified her that her date of birth was also compromised in the Data Breach.

113. Plaintiff Viruet has suffered several varieties of actual injuries as a result of the Data Breach.

114. After she received the Notice Letter from Defendant, Plaintiff determined that her PII was found on the dark web. Her PII can be purchased by criminals intending to utilize the PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; or file false unemployment claims. Plaintiff Viruet believes that the availability of her PII on the dark web is directly related to the Data Breach.

115. In addition, Plaintiff Viruet has also experienced a substantial increase in suspicious emails and "spam" telephone calls since the Data Breach which she believes were a result of the Data Breach.

116. Moreover, as a result of the Data Breach and the directives that she received in the Notice Letter, Plaintiff has already spent precious hours dealing with the consequences of the Data Breach (*e.g.*, self-monitoring her bank and credit accounts), as well as her time spent verifying the legitimacy of the Notice of Data Breach, communicating with her bank, researching and purchasing multiple forms of security protection services. This time has been lost forever and cannot be recaptured. Moreover, Plaintiff spent this time at Defendant's direction. Indeed, in the notice letter Plaintiff received from Defendant, Defendant directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and credit reports for any unauthorized activity." Given the short timeframe the attempted identity theft occurred in from the time of the Data Breach, it is reasonable to expect that Plaintiff will continue to have to devote significantly more precious time and resources to the aftermath of the Data Breach for many years to come. To date, she has already spent at least 10 hours dealing with the consequences of the Data Breach.

117. Plaintiff has suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and deprivation in the value of her PII, a form of property that Defendant obtained from the Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

118. Plaintiff also lost the benefit of the bargain she struck with CSS and suffered price premium damages for the services she paid for. Had she known that CSS would had inadequate data security practiced, she would not have entered into a business transaction with Defendant, paid for Defendant's services, or provided her PII to Defendant.

119. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach since she received the Notice Letter. Plaintiff is especially concerned about the theft of her full name paired with her Social Security number and date of birth, which is readily obtainable from the driver's license that CSS notified her may have been stolen in the Data Breach.

120. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

121. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in CSS's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

122. Plaintiff brings this Complaint on behalf of herself and the Class Members pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and (c)(4).

123. Plaintiff seeks to remedy those harms described herein on behalf of herself and all similarly situated persons whose PII was accessed unlawfully during the Data Breach.

124. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons residing in the United States whose PII was compromised in the Data Breach (the "Nationwide Class" or the "Class").**

125. The Nationwide Class asserts claims under New Jersey law against CSS for: (1) negligence, (2) negligence *per se*, (3) breach of confidence, (4) intrusion upon seclusion, (5) breach of implied contract, (6) unjust enrichment, (7) violations of New Jersey state consumer protection statutes; and (8) Declaratory Judgment.

126. Excluded from the Nationwide Class are CSS, any entity in which either CSS has a controlling interest, and either CSS's officers, directors, legal representatives, successors, subsidiaries, and agents; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and any and all federal, state or local governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions. Also excluded from the Nationwide Class are any judicial officers presiding over this matter, members of their immediate family, and members of their judicial staff.

127. Numerosity, Fed R. Civ. P. 23(a)(1): The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Nationwide Class consists of over 66,000 individuals whose sensitive data was compromised in the Data Breach.

128. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

(a) Whether CSS breached a duty to Class Members to safeguard their PII;

(b) Whether CSS expressly or impliedly promised to safeguard the PII of Plaintiff and Class Members;

(c) Whether CSS unlawfully used, maintained, lost, or disclosed Plaintiff 's and Class Members' PII;

(d) Whether CSS failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(e) Whether CSS's data security systems prior to, during, and after the Data Breach complied with the applicable FTC data security laws and regulations;

(f) Whether CSS's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

(g) Whether unauthorized third parties accessed or obtained Class Members PII in the Data Breach;

(h) Whether the CSS knew or should have known that its data security systems and monitoring processes were deficient;

(i) Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the CSS's misconduct;

(j) Whether CSS's conduct was negligent;

(k) Whether CSS breached an expressed of implied contractual obligations;

(l) Whether CSS violated New Jersey state consumer protections statutes;

(m) Whether CSS was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;

(n) Whether CSS failed to provide notice of the Data Breach in a timely manner;

(o) Whether CSS adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur; and

(p) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

129. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

130. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff 's counsel are competent and experienced in litigating class actions and data breach cases.

131. Predominance, Fed. R. Civ. P. 23(b)(3): CSS has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff 's and Class Members' data

was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from CSS's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

132. Superiority, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for CSS. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

133. Manageability, Fed. R. Civ. P. 23(b)(3): The litigation of the claims brought herein is manageable. CSS's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in CSS's records.

134. Conduct Generally Applicable to the Class, Fed. R. Civ. P. 23(b)(2): Further, CSS has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate. Unless a class-wide injunction is issued, CSS may continue in its failure to properly

secure the PII of Class Members, CSS may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and CSS may continue to act unlawfully as set forth in this Complaint.

135. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. The particular issues include, but are not limited to:

(a) Whether CSS owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(b) Whether CSS breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(c) Whether CSS failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

(d) Whether an implied contract existed between CSS on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

(e) Whether CSS breached the implied contract;

(f) Whether CSS adequately, and accurately informed Plaintiff and Class Members that their PII had been compromised;

(g) Whether CSS failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(h) Whether CSS engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and

(i) Whether Class Members are entitled to actual damages, statutory damages, nominal damages, injunctive relief, and/or punitive damages as a result of CSS's wrongful conduct.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

136. Plaintiff repeats the allegations contained in paragraphs 1 through 189 as if fully set forth herein.

137. Plaintiff brings this Count on behalf of herself and the Nationwide Class.

138. CSS owed several common law duties to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff 's and Class Members' PII within its control from being accessed, compromised, exfiltrated, and stolen by criminal third parties in foreseeable cyber-crimes.

139. First, a common law duty arose by the foreseeability of the cyber-crimes. Due to the ongoing threat and highly publicized cyber-attacks businesses like CSS that acquire and store PII, CSS was on notice of the substantial and foreseeable risk of a cyber-attack on its systems, and that Plaintiff and Class Members would be harmed if CSS did not protect Plaintiff 's and Class Members' information from threat actors.

140. CSS knew or should have known that its systems were vulnerable to unauthorized access and exfiltration by criminal third parties. CSS knew, or should have known, of the importance of safeguarding Plaintiff 's and Class Members' PII – including Social Security numbers, driver's license numbers, and financial account information. CSS further knew or should have known and of the foreseeable consequences and harm to Plaintiff and Class Members, if CSS's data security system and network was breached – including, specifically, the risk of identity theft and related costs imposed on Plaintiff and Class Members as a result of a data breach. CSS knew or should have known about these risk and dangers to Plaintiff and Class Members and taken steps to strengthen its data, IT, and email handling systems accordingly.

141. Second, by obtaining, collecting, using, retaining, and deriving benefits from Plaintiff 's and the Class Members' PII, Defendant assumed the legal duty to protect Plaintiff 's and Class Members' PII from foreseeable cyber-crimes.

142. Third, CSS's duty to use reasonable data security measures arose as a result of the special relationship that existed between CSS and the Plaintiff and Class Members. The special relationship arose because CSS received Plaintiff 's and Class Members' confidential data as part of the financial process for obtaining products or services. CSS was in the sole position to ensure that it had sufficient safeguards to protect against the harm to Plaintiff and Class Members that would result from a data breach.

143. Finally, CSS's duties arose by statute under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair or deceptive acts or practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of CSS's duty.

144. CSS breached its respective common law and statutory duties by failing to provide data security consistent with industry standards to ensure that its systems and networks adequately protected the PII it had been entrusted against foreseeable cyber-crimes. CSS did not use reasonable security procedures and practices appropriate for the nature of the sensitive information it was maintaining, causing Plaintiff 's and Class Members' PII to be exposed. As a result, CSS increased the risk to Plaintiff and Class Members that their PII would be compromised and stolen in a cyber-crime.

145. Plaintiff 's and Class Members' PII would not have been compromised in the Data Breach but for CSS's wrongful and negligent breach of its duties.

146. Neither Plaintiff nor, upon information and belief, the other Class Members contributed to the Data Breach or subsequent misuse of their PII as described in this Complaint.

147. CSS breached its obligations to Plaintiff and the Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Upon information and belief, CSS could have prevented this Data Breach by encrypting, or adequately encrypting, or otherwise protecting its equipment and computer files containing Plaintiff 's and Class Members' PII.

148. Upon information and belief, CSS's negligent conduct also includes, but is not limited to, one or more of the following acts and omissions:

(a) Failing to maintain and update an adequate data security system to reduce the risk of data breaches;

(b) Failing to adequately train employees to protect consumers' PII;

(c) Failing to adequately monitor, evaluate, and ensure the security of its network and systems;

(d) Failing to properly monitor its own data security systems for existing intrusions;

(e) Failing to comply with the minimum FTC guidelines for cybersecurity, in violation of the FTCA;

(f) Failing to adhere to industry standards for cybersecurity;

(g) Failing to encrypt or adequately encrypt the PII;

(h) Failing to implement reasonable data retention policies;

(i) Failing to timely and adequately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed; and

(j) Was otherwise negligent.

149. Furthermore, CSS was plainly aware that it should destroy any PII that it no longer needed to provide products or services or at least should have ensured extra precautions to secure

such PII since, under such circumstances, there was effectively no longer a "legitimate business 'need to know'" for accessing it.

150. As a direct and proximate result of Defendant's negligent acts and/or omissions, Plaintiff 's and Class Members' PII was compromised, and they are all at a high risk of identity theft and financial fraud for many years to come. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) invasion of privacy; (b) financial costs incurred mitigating the risk of future identity theft; (c) loss of time and loss of productivity incurred mitigating the risk of future identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; and (f) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff 's and Class Members' Sensitive Information.

151. Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of herself and all similarly situated persons whose Sensitive Information were compromised as a result of the Data Breach. Plaintiff seeks compensatory damages for invasion of privacy, loss of time, opportunity costs, out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

152. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that CSS's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Nationwide Class)

153. Plaintiff repeats the allegations contained in paragraphs 1 through 152 as if fully set forth herein.

154. Plaintiff brings this Count on behalf of herself and the Nationwide Class.

155. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as CSS, of failing to use reasonable measures to protect PII. 15 U.S.C. §45(a)(1).

156. The FTC publications and orders described above also form part of the basis of CSS's duty in this regard.

157. CSS violated the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards. CSS's conduct was particularly unreasonable given the nature and amount of PII it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as CSS, including, specifically, the immense damages that would result to Plaintiff and Class Members.

158. CSS's violations of the FTCA, as interpreted by the FTC to include a duty to employ adequate and reasonable data security measures, constitute negligence *per se*.

159. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

160. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

161. As a direct and proximate result of CSS's negligence *per se* under the FTCA, Plaintiff and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT III
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Nationwide Class)

162. Plaintiff repeats the allegations contained in paragraphs 1 through 161 as if fully set forth herein.

163. Plaintiff brings this Count on behalf of herself and the Nationwide Class.

164. CSS and Plaintiff and Class Members maintained a confidential relationship, whereby CSS undertook a duty not to disclose the PII provided to CSS to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

165. CSS knew Plaintiff 's and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII they collected, stored, and maintained.

166. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because CSS failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

167. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

168. As a direct and proximate result of CSS's breach of confidence, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seeks an award of nominal damages.

COUNT IV
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Nationwide Class)

169. Plaintiff repeats the allegations contained in paragraphs 1 through 168 as if fully set forth herein.

170. Plaintiff brings this Count on behalf of herself and the Nationwide Class.

171. CSS intentionally intruded into Plaintiff 's and Class Members' seclusion by failing to keep their PII secure.

172. By failing to keep Plaintiff 's and Class Members' PII secure, and allowing for access and disclosing of the PII to unauthorized parties for unauthorized use, CSS unlawfully invaded Plaintiff 's and Class Members' privacy right to seclusion by, *inter alia*:

(a) intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

(b) invading their privacy by improperly using their PII properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

(c) failing to adequately secure their PII from disclosure to unauthorized persons; and

(d) enabling the disclosure of their PII without consent.

173. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial, employment, and personal information.

174. Plaintiff and Class Members reasonably expected this information to remain confidential, Defendant allowed an unauthorized actor to access this information, and the disclosure of this information would be and is highly offensive to a reasonable person.

175. As a direct and proximate result of CSS's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seeks an award of nominal damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

176. Plaintiff repeats the allegations contained in paragraphs 1 through 175 as if fully set forth herein.

177. Plaintiff brings this Count on behalf of herself and the Nationwide Class in the alternative to all other Counts alleged herein.

178. For years and continuing to today, CSS's business model has depended upon it being entrusted with customers' PII. Trust and confidence are critical and central to the services provided by CSS in the home healthcare industry. Unbeknownst to Plaintiff and Class Members, however, CSS did not secure, safeguard, or protect its customers' PII and employed deficient security procedures and protocols to prevent unauthorized access to customers' PII. CSS's deficiencies described herein were contrary to its security messaging.

179. Plaintiff and absent Class Members received services from CSS or its affiliates, and CSS was provided with, and allowed to collect and store, their PII on the mistaken belief that CSS complied with its duties to safeguard and protect its customers' PII. Upon information and belief, putting its short-term profit ahead of safeguarding PII, and unbeknownst to Plaintiff and Class Members, CSS knowingly sacrificed data security in an attempt to save money.

180. Upon information and belief, CSS knew that the manner in which they maintained and transmitted customer PII violated industry standards and their fundamental duties to Plaintiff and Class Members by neglecting well-accepted security measures to ensure confidential information was not accessible to unauthorized access. CSS had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

181. CSS had within its exclusive knowledge, and never disclosed, that they had failed to safeguard and protect Plaintiff 's and Class Members' PII. This information was not available to Plaintiff, Class Members, or the public at large.

182. CSS also knew that Plaintiff and Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and other personal information.

183. Plaintiff and Class Members did not expect that CSS would knowingly insecurely maintain and hold their PII when that data was no longer needed to facilitate a business transaction or other legitimate business reason. Likewise, Plaintiff and Class Members did not know or expect that CSS would employ substantially deficient data security systems and fail to undertake any required monitoring or supervision of the entrusted PII.

184. Had Plaintiff and Class Members known about CSS's efforts to deficiencies and efforts to hide its ineffective and substandard data security systems, Plaintiff and Class Members would not have entered into business dealings with CSS.

185. By withholding the facts concerning the defective security and protection of customer PII, CSS put their own interests ahead of the very customers who placed their trust and confidence in CSS and benefitted it to the detriment of Plaintiff and Class Members.

186. As a result of its conduct as alleged herein, CSS sold more services and products than it otherwise would have and was able to charge Plaintiff and Class Members more for CSS's services than it otherwise could have. CSS was unjustly enriched by charging for and collecting for those services that it would not have obtained to the detriment of Plaintiff and Class Members.

187. It would be inequitable, unfair, and unjust for CSS to retain these wrongfully obtained fees and benefits. CSS's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

188. CSS's unfair and deceptive conduct to not disclose those defects have, among other things, caused Plaintiff and Class Members to enter a business arrangement that was deceptive and dangerous to their identities.

189. As a result, Plaintiff and Class Members paid for services that they would not have paid for had Defendant disclosed the inadequacy of its data security practices.

190. Plaintiff and each Member of the proposed Class are each entitled to restitution and non-restitutionary disgorgement in the amount by which CSS were unjustly enriched, to be determined at trial.

COUNT VI
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

191. Plaintiff repeats the allegations contained in paragraphs 1 through 190 as if fully set forth herein.

192. Plaintiff brings this Count on behalf of herself and the Nationwide Class.

193. When Plaintiff and Class Members paid money and provided their PII to CSS in exchange for goods or services, they entered into implied contracts with CSS pursuant to which CSS agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

194. CSS solicited and invited prospective customers to provide their PII as part of its regular business practices. As a condition of receiving services, Defendant required Plaintiff and Class Members to provide their PII, including full names, Social Security numbers, passport

numbers, addresses, dates of birth, and driver's license number and other governmental identification numbers.

195. Pursuant to FTC guidelines and standard practice in the financial industry, CSS was obligated to take reasonable steps to maintain the security of Plaintiff 's and Class Members' PII. As a result, by requesting that Plaintiff and Class Members provide their PII as part of their doing business with CSS, CSS implicitly promised to adhere to these industry standards.

196. Plaintiff and Class Members each accepted CSS's offers and provided their PII to CSS. In entering such implied contracts, Plaintiff and the Class reasonably believed that CSS's data security practices and policies were reasonable and consistent with industry standards, and that CSS would use part of the fees received from Plaintiff and the Class to pay for adequate and reasonable data security practices to safeguard the PII.

197. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant. Defendant accepted the PII, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII confidential.

198. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

199. Plaintiff and the Class would not have entered into transactions with CSS if Plaintiff had known that CSS would not protect their PII.

200. Plaintiff and the Class would not have provided and entrusted their PII to CSS in the absence of the implied contract between them and CSS to keep the information secure.

201. Plaintiff and the Class fully performed their obligations under the implied contracts with CSS.

202. CSS breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

203. As a direct and proximate result of CSS's breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

COUNT VII
NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-2
(On Behalf of Plaintiff and the Nationwide Class)

204. Plaintiff repeats the allegations contained in paragraphs 1 through 203 as if fully set forth herein.

205. Plaintiff brings this Count on behalf of herself and the Nationwide Class.

206. The New Jersey Consumer Fraud Act ("New Jersey CFA") makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby." N.J.S.A. § 56:8-2.

207. By the acts and conduct alleged herein, CSS committed unfair or deceptive acts and practices by:

(a) failing to maintain adequate computer systems and data security practices to safeguard PII;

(b) failing to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

(c) continuing to gather and store PII, and other personal information after CSS knew or should have known of the security vulnerabilities of its computer systems that were exploited in the data breach;

(d) continuing to gather and store PII, and other personal information after CSS knew or should have known of the Data Breach and before CSS allegedly remediated the data security incident;

(e) continuing to store and maintain the PII of former customers when CSS had no legitimate business need to do so; and

(f) delaying in notifying the Plaintiff and Class Members of the Data Breach, and the full scope of the Data Breach.

208. These unfair acts and practices violated duties imposed by laws, including, but not limited to the FTCA, the New Jersey Deceptive and Unfair Trade Practices Act, and the New Jersey CFA.

209. CSS's delay in notifying the victims of the Data Breach also violates provisions of the New Jersey Consumer Security Breach Disclosure Act, which required CSS, once it knew or had reason to know of a data security breach involving personal information, to provide prompt and direct notice of such breach to any affected, indicating another deceptive act and practice.

210. The foregoing deceptive acts and practices emanated from New Jersey and were directed at consumers/purchasers in New Jersey and in each state where Defendant did business.

211. CSS, Plaintiff, and Class Members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

212. CSS engaged in "sales" of "merchandise" within the meaning of N.J.S.A. § 56:8-1(c), (d).

213. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the financial services provided, specifically as to the safety and security of PII, and other personal and private information, to induce consumers to purchase the same.

214. CSS's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Class Action Complaint are material in that they relate to matters

which reasonable persons, including Plaintiff and Members of the Class, would attach importance to in making their purchasing decisions or conducting themselves regarding the purchase of services from CSS.

215. Plaintiff and Class Members are consumers who made payments to Defendant for the furnishing of medical related services that were primarily for personal, family, or household purposes.

216. CSS engaged in the conduct alleged in this Complaint, entering transactions intended to result, and which did result, in the furnishing of services to consumers, including Plaintiff and Class Members. CSS's acts, practices, and omissions were done in the course of CSS's business of marketing, offering to sell, and furnishing services from the State of New Jersey. As a direct and proximate result of CSS's multiple, separate violations of N.J.S.A. § 56:8-2, Plaintiff and the Class Members suffered damages including, but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in CSS's possession and is subject to further unauthorized disclosures so long as CSS fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of CSS's services they received.

217. Also as a direct result of CSS's violation of the New Jersey CFA, Plaintiff and the Class are entitled to damages as well as injunctive relief, including, but not limited to, ordering CSS to: (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members. Plaintiff and Class Members were injured because: (a) they would not have paid for Defendant's services had they known the true nature and character of CSS's data security practices; (b) would not have entrusted their PII to CSS in the absence of promises that Defendant would keep their information reasonably secure, and (c) would not have entrusted their PII to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

218. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

219. On behalf of herself and other members of the Class, Plaintiff and Class Members are entitled to recover legal and/or equitable relief, including an order enjoining CSS's unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J.S.A. § 56:8-19, and any other just and appropriate relief.

COUNT VIII
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class)

220. Plaintiff repeats the allegations contained in paragraphs 1 through 219 as if fully set forth herein.

221. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

222. Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiff and Class Members.

223. Defendant owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PII.

224. Defendant still possesses PII regarding Plaintiff and Class Members

225. Since the Data Breach, Defendant has announced few if any specific and significant changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

226. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

227. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

228. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

229. Plaintiff and Class Members, therefore, seeks a declaration: (a) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (b) that to comply with its contractual obligations and duties of

care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

(a) Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

(b) Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

(c) Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

(d) Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

(e) Ordering that Defendant not transmit PII via unencrypted email;

(f) Ordering that Defendant not store PII in email accounts;

(g) Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

(h) Ordering that Defendant conduct regular computer system scanning and security checks;

(i) Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

(j) Ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and her counsel to represent the certified Class;

B. For equitable relief enjoining CSS from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff 's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting CSS from engaging in the wrongful and unlawful acts described herein;

ii. requiring CSS to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring CSS to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless CSS can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring CSS to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff 's and Class Members' personal identifying information;

v. prohibiting CSS from maintaining Plaintiff 's and Class Members' PII on a cloud-based database;

vi. requiring CSS to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on CSS's systems on a periodic basis, and ordering CSS to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring CSS to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring CSS to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring CSS to segment data by, among other things, creating firewalls and access controls so that if one area of CSS's network is compromised, hackers cannot gain access to other portions of CSS's systems;

x. requiring CSS to conduct regular database scanning and securing checks;

xi. requiring CSS to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xii. requiring CSS to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring CSS to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with CSS's policies, programs, and systems for protecting PII;

xiv. requiring CSS to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor CSS's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring CSS to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring CSS to implement logging and monitoring programs sufficient to track traffic to and from CSS's servers; and

xvii. for a period of ten years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate CSS's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

A jury trial is demanded by Plaintiff and the putative Class Members as to all issues so triable.

Respectfully Submitted,

/s/ Victoria Maniatis
Victoria Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza,
Suite 500
Garden City, NY 11530
Tel.: 516-741-5600
VManiatis@milberg.com

Gary M. Klinger
David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

Terence R. Coates*
Justin C. Walker*
Jonathan T. Deters*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
jdeters@msdlegal.com

**pro hac vice forthcoming*

Attorneys for Plaintiff and the Proposed Class